INDIUM

Data Governance & Data Assurance

- Good Decisions Need Both

E-BOOK

Discover WHAT, WHY, HOW, WHO & Top Emerging Practices of Data Governance & Security for the Modern Enterprise

You do not always need to tell someone that something is the “talk of the town” because you know it is! In the vast digital landscape, imagine your business as a mighty ship sailing through treacherous waters.

Your ship carries valuable cargo, a treasure chest overflowing with gold and jewels. This treasure represents your data, a precious asset with immense value and success. However, in this vast ocean of data, storms of uncertainty and pirates of cyber threats lurk, ready to plunder your treasure. To safeguard your bounty and harness its true power, you need a skilled crew and a robust system of governance.

Enter The Helm of Enterprise Data Governance – a sturdy compass that steers your ship, ensuring your data’s quality, security, and usability. With data governance as your guiding star, you can chart a course toward transformative opportunities and reach the shores of digital triumph.

To See is To Believe

The Open Data Institute’s research by Metia Group reveals a growing need for recognized standards, codes of conduct, and tools for managing data risk.

66% of respondents feel that the current data assurance supply does not fully meet their needs.

The assurance of external data is expected to grow significantly, with 98% of service providers predicting this trend.

71% of data users in Western Europe are particularly interested in external data assurance.

Increasing market demand for data sharing is driving the growth of external data assurance, according to 63% of respondents.

The data assurance products and services market was estimated to be worth **$3.5 billion in 2022** and is projected to reach $5.6 billion by 2027.

Not Only But Also!

According to Gartner, 80% of organizations scaling digital business may fail by 2025 without a modern approach to data governance.

Harvard Business Review Analytic Services statistics highlight the importance of addressing the evolving risks of digital transformation and emphasize the need for organizations to prioritize data governance for successful outcomes.

92% of business leaders surveyed believe that shifting business models associated with digital transformation creates new risk types.

77% of respondents consider robust security, risk, and compliance strategy essential for business success.

Surprisingly, 53% of organizations have not yet developed a robust, business-wide data governance approach.

So, how can you close this gap and implement data governance to benefit your business? How does data assurance increase confidence in data? How does data assurance support data governance – the policies, processes, people, standards, and technologies governing access to data assets?

This eBook will delve into the significance of data governance in today's business landscape and its crucial role in ensuring data quality, particularly in the context of advancing technologies like Machine Learning and AI. By exploring enterprise data governance, we aim to enlighten stakeholders and highlight its relevance to achieving company objectives.

Down to Business

Let's not make things complicated. A quick Google search will inundate you with numerous definitions regarding data assurance. However, at Indium, we are big fans of keeping things simple.

So, we asked Srikanth Manoharan, Executive Vice President of QA Digital Assurance, and Arunachalam Sankaralingam, Vice President of Digital Assurance - **"What is Data Assurance?"**

Data gets created, moved, and transformed, but when the data moves/transformed to a different destination, the art of ensuring the correctness of the data is Data assurance. We are not talking just 1 bit of data, but rather zillions of data.

Srikanth Manoharan,
Executive Vice President of QA Digital Assurance

In the current digital age, executives make decisions relying on the data, which has increased exponentially. Data assurance is crucial for this reason, and the key is to focus on ensuring the accuracy, integrity, availability, and confidentiality of data within an enterprise. It also includes validation practices to safeguard data against unauthorized access, corruption, loss, and other potential risks.

Arunachalam Sankaralingam,
Vice President of Digital Assurance

The collaborative research conducted by Metia Group and the Open Data Institute (ODI) sheds light on the comprehensive definition of data assurance, encompassing service providers, data holders, and data users.

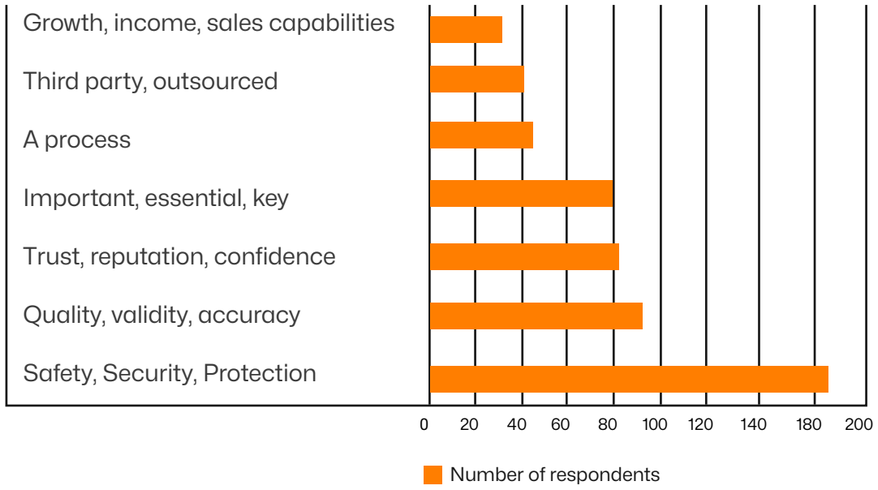
What is Data Assurance?

Data Assurance is Associated with Quality Information and Business Confidence

> *The purpose of external data assurance goes beyond a statement from a third party that the contents of a report are true based on certain principles; it enhances confidence about the integrity of information and of underlying operational processes and improves the quality of an organisation's decision-making process.*
>
> UK, data holder

> *Data assurance means quality control on the data intake and structuring, guidelines and guardrails for responsible and effective use of the data, and safety and security of our most sensitive data and data providers' privacy.*
>
> UK, data holder

USERS' ATTITUDES TOWARDS DATA ASSURANCE DEFINITION



Source: Metia, Data Assurance Survey

Q: Please describe what data assurance means to you in your own words. N=651

In Data We Trust! What's Involved In Data Assurance?

Data assurance encompasses practices that span the lifecycle of data usage within an organization, covering collection, storage, and utilization, considering both technical and human aspects.

Data Quality | Ensuring the accuracy and reliability of data is essential for effective decision-making. Data assurance practices encompass data validation and continuous data quality monitoring.

Ensuring the absence of missing, incomplete, or erroneous entries in the data is crucial to prevent inaccurate analysis, reporting, and decision-making. | **Data Completeness**

Data Integrity | Guaranteeing that data remains accurate, consistent, and unaltered during storage, processing, and transmission. This objective can be accomplished through the use of checksums, hash functions, digital signatures, and robust data validation procedures.

A guiding framework that aligns data usage with business objectives, incorporating trust concepts to enhance data | **Data Strategy**

Data Governance | Ensuring controlled and secure access to data, following company policies and external regulations, and addressing ethical and cultural dimensions often overlooked by traditional governance plans.

Striking a balance between deriving value from data and avoiding detrimental impacts, focusing on aligning data usage with societal and organizational values beyond regulatory compliance. | **Data Ethics**

Data Culture | The mindset and work practices that foster effective data utilization, particularly emphasizing data-informed decision-making as a key feature for building trust and promoting data assurance practices.

Trust as an outcome - The ultimate goal of data assurance, wherein organizations prioritize trustworthiness in their data practices, incorporating these diverse practices to foster a culture of trust and confidence.

Don’t Get Flummoxed by Data Governance. Get Focused

Data governance begins with data discovery and defining the principles, policies, best practices, standards, guidelines, and rules with the data across the organization while securing the data and complying with data privacy laws and other regulations.

Krishnakumar Aravamudhan,
Vice President - Data Management

Organizations to keep a longer-term vision and clear road map with Data Governance at the same time can be started small. It is a continuous process of monitoring and controlling. With the successful implementation of data governance, the organization benefits from the unified\common data model, which eliminates unwanted data, focuses on the right data, has the data definitions, data cataloging aids the data implementation built efficient, reliable, accurate, and supports to take timely business decisions.

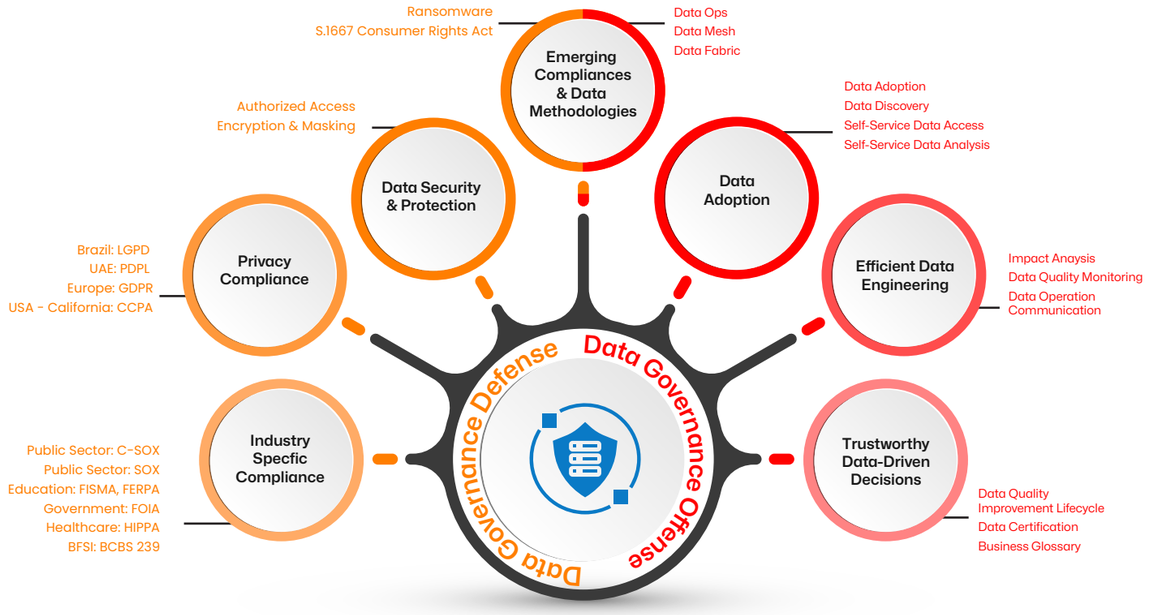
Rajavel Kanagavelu,
Senior Data Architect - Data Management

Data Governance encompasses the processes and procedures organizations employ to manage, utilize, and safeguard their data assets, encompassing digital and physical formats. A fundamental best practice in data governance is defining the meaning and significance of data within the organization, enabling strategic utilization for business advancement.

Imagine data governance as the comprehensive framework encompassing the who, what, when, where, and why of your organization’s data, providing a holistic perspective on its management. The rapid evolution of security frameworks & regulations like GDPR, CPRA, CCPA, PIPL, LGPD, ISO, NIST, and more, requires organizations to prioritize robust data governance. Given the prevalence of data breaches and the continuous evolution of regulations like HIPAA, GDPR, and CCPA, data governance plays a crucial role in safeguarding customers’ and citizens’ private information.

For example: In the context of digital payments, when individuals engage in digital transactions, they share sensitive personal and banking details with applications, devices, and various other modes facilitated by Banking and Financial Services companies. These financial institutions must safeguard this sensitive data from unauthorized access, protect it from hackers, and comply with Banking and Financial services regulations, such as PCI DSS, GDPR, and many others. Data governance plays a crucial role in ensuring that the organization's data remains safe and secure while adapting to changes in rules, regulations, tools, and technology. It enables effective implementation and management of data protection measures and caters to the dynamic nature of these changes.

Experts' Insights: Balancing Defensive and Offensive Approaches in Data Governance for Financial Institutions



Organizations tend to adopt a defensive approach due to the necessity of adhering to regulations, privacy laws, and industry-specific compliances. This approach ensures the protection of customer data from unauthorized access, cyber threats, and attacks. However, solely focusing on defense might lead to overlooking the importance of data and the potential value it can bring to both the business and customers.

On the other hand, an offensive approach emphasizes adding business value to the organization, customers, and stakeholders. This is achieved through various strategies:

1. Modernizing Data Governance platforms by incorporating AI and ML technologies to enhance data management processes.
2. Embracing emerging tools and technologies and establishing the right framework and technological architecture to meet the current and future needs of the organization.
3. Adapting to cloud technologies, enabling real-time data analytics, and promoting self-service business intelligence.

Speed Bump! Unraveling Common Challenges in Data Governance

Within organizations, poor data governance can arise from a variety of issues. While some challenges may be more apparent, each one is fixable. Let's delve into some of these common hurdles:

Supply lens

THE LACK OF QUALITY CONTROL AND DATA GOVERNANCE ARE SEEN AS KEY PAIN POINTS BY DATA ASSURERS

SERVICE PROVIDERS ATTITUDES TOWARDS KEY PAIN POINTS ON THE DEMAND SIDE

50%

Data quality control:
Assuring that external data is reliable and of high quality

Data management and governance:
Assuring that external data is consistently managed and governed in line with regulation and internal procedures enabling trust and reliability

33%

Data compliance:
Assuring that external data is conforming to all major regulations, including GDPRa, CCPA, DSAR, etc.

Collection and sourcing:
Assuring that external data collected and sourced in ethical and equitable manner

Data curation:
Assuring that external data is maintained, updated and cleansed in a trustworthy manner

31%

Data harmonisation:
Assuring that external data and underlying practices conform to existing standards

30%

Data exploitation:
Assuring that external data provides trustworthy insight, enabling decision making

26%

Data interlinking:
Assuring that external data is consistent with other sources and does not create ethical

24%

Data sharing/publishing:
Assuring that external data is 'fit for sharing'

Source: Metia, Data Assurance survey

Q: In your opinion, what are the key pain-points that external data assurance users/holders are looking to solve/Improve today? Please select all relevant answers, N=141

Control of data:

Despite multiple data collection systems and applications, many companies lack effective controls to govern data quality. Inconsistencies between systems lead to incomplete, variable, or misaligned data.

Adding or moving systems:

The desire for quick task completion can lead to hasty system implementation or migration in the fast-paced business world. Rushing these processes often results in the inadequate establishment of controls and parameters. Delaying these crucial guidelines further exacerbates data quality issues and may hinder necessary adjustments.

Aging systems:

Over time, data-gathering and maintenance systems can deteriorate in functionality. While they may still gather information, they may lack the necessary capabilities for insightful analysis and timely decision-making.

Employee turnover:

In certain organizations, only a few employees possess knowledge of data collection, access to collection tools, and understanding of control establishment and maintenance. If these key individuals depart, the company may face challenges in making adjustments and resolving potential issues. Data collection processes should evolve with changing customer bases and new data requirements, making it vital for remaining employees to grasp the systems and processes involved.

Lack of visibility into data:

Data and ongoing trend analysis are vital for informed decision-making and understanding each team's workload. Many companies face siloed data ingestion and consumption processes due to a lack of visibility into available information. Without a clear structure, a consistent data and reporting catalog, and defined standard processes for data usage, organizational processes become isolated, resulting in diminished trust, heightened frustration, and the inability to make informed decisions swiftly.

Pros and Cons of Data Governance

Effective data governance is crucial for organizations to ensure consistency and accuracy in their systems and data. Inconsistencies can persist across different departments and systems without proper data governance, leading to various challenges. For instance, customer accounts may be recorded in various formats within sales, logistics, and customer service systems. This lack of uniformity can complicate data integration efforts and give rise to data integrity issues, ultimately impacting the accuracy of crucial business intelligence (BI), enterprise reporting, and analytics applications. Furthermore, data errors may go unnoticed and unresolved, compromising BI and analytics' precision.

Implementing best practices in data governance offers several concrete advantages, enabling organizations to maximize the value of their data while mitigating operational and analytic issues arising from inconsistencies. Some key benefits include:

Advantages	Concerns / Considerations
Reduced IT costs related to data governance through centralized policies and systems.	Implementation requires a company-wide mandate, making it a large and complex project.
Better cross-functional decision-making and communication enabled by data standards.	Resources and focus from various teams are needed, potentially diverting attention from other efforts.
Easier management of compliance audits and standards maintenance.	Coordination with broader IT governance policies is necessary to ensure alignment and consistency.
Enhanced business intelligence for short and long-term planning, including mergers and acquisitions.	Gaining employee buy-in can be challenging, requiring incentives and motivation to foster compliance.
Controlled and organized data growth.	Data governance efforts must be flexible to accommodate team needs and user-friendly to promote adoption
Streamlined adaptation to new data and privacy legislation.	The complex implementation of technology and tools for effective data governance requires careful selection based on strategy and guidance from reliable sources like Gartner, G2 and more.

Key Components of Enterprise Data Governance with Data Assurance

As shared by industry experts Srikanth Manoharan, Executive Vice President of QA Digital Assurance, and Arunachalam Sankaralingam, Vice President of Digital Assurance from Indium Software, here's how Data Assurance further helps in Data Governance through the following angles:

> *Data assurance is not only about testing, but governance is also key. Different teams could be involved in developing and deploying solutions to meet customer needs.*

Arunachalam Sankaralingam,
Vice President of Digital Assurance

1. Data Lineage and Traceability:

Data Assurance establishes data lineage, tracing the origin, transformation, and movement of data throughout its lifecycle. This ensures transparency and accountability, allowing organizations to understand how data is used and modified.

2. Data Cataloging and Metadata Management:

Data Assurance facilitates data cataloging and metadata management. Organizing and describing data assets makes it easier for stakeholders to discover, understand, and utilize relevant data efficiently.

3. Data Access Control and Governance:

Data Assurance enforces data access controls aligned with Data Governance policies. It ensures that only authorized personnel can access specific data sets, maintaining data confidentiality and reducing the risk of data breaches.

4. Data Retention and Deletion Policies:

Data Assurance helps design and implement data retention and deletion policies. This ensures that data is retained for the required duration per regulations and appropriately disposed of when it is no longer needed, reducing data storage costs and compliance

5. Data Versioning and Change Management:

Data Assurance manages data versioning and change control processes. It tracks data changes, maintains historical records, and ensures proper version control, enabling data users to understand data evolution accurately.

6. Data Governance Tools and Technologies:

Data Assurance selects and deploys suitable Data Governance tools and technologies. This includes data governance platforms, data quality tools, data monitoring solutions, and data lineage tools, optimizing Data Governance processes.

7. Data Governance Education and Training:

Data Assurance provides education and training on Data Governance best practices. This helps staff members understand the importance of data compliance and promotes a data-centric culture across the organization.

8. Data Incident Management and Resolution:

Data Assurance is involved in data incident management, promptly detecting and responding to data-related issues. It aids in data breach investigations, recovery procedures, and implementing preventive measures.

9. Data Compliance Reporting:

Data Assurance prepares data compliance reports for regulatory bodies and internal stakeholders. These reports detail data management activities, data quality, and adherence to Data Governance policies.

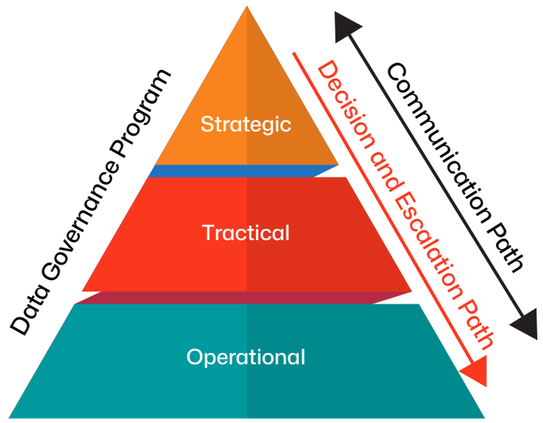
10. Data Governance Performance Measurement:

Data Assurance establishes key performance indicators (KPIs) to measure the effectiveness of Data Governance initiatives. This allows organizations to continually improve their data management practices.

By focusing on these technical aspects, Data Assurance helps strengthen Data Governance practices, enhances data accountability, and ensures data-driven decision-making, fostering a culture of data excellence within the organization.

Who Is Responsible for Data Governance?

The organization (the “where” and “who”)
Business aspects (the “what”)
Technical aspects (the “how”).



Data Governance Levels

Data governance involves various organizational stakeholders, each crucial in ensuring effective governance. Let’s explore the key stakeholders involved in data governance:

Who's part of the program on data governance?

2

DATA GOVERNANCE COUNCIL OR COMMITTEE
Typically made up of executives from all business units, it sets data policies and standards and resolves issues.

3

DATA GOVERNANCE TEAM
A data governance manager heads a program office that may also include data architects and governance specialists.

4

DATA STEWARDS
Stewards oversee data sets and are in charge of implementing governance policies and monitoring compliance with them.

1

DATA GOVERNANCE TEAM
A data governance manager heads a program office that may also include data architects and governance specialists.

5

DATA QUALITY ANALYSTS AND ENGINEERS
They work with the governance team and data stewards to fix data errors and track data quality metrics.

CDO (Chief Data Officer): A CDO oversees all data operations. They supervise technology and process deployment, data management, governance, and analytics procedures.

Data Owners: These individuals are responsible for making critical decisions regarding data and enforcing them across the organization. Data owners can be appointed at different levels, such as entity level (e.g., customer records, product records, employee records) and attribute level (e.g., customer address, product classification). They hold ultimate accountability for the overall condition of data as a valuable asset.

Data Stewards: Data stewards are the guardians of data policies and standards in daily business operations. They often possess expertise in specific data entities or attributes and ensure adherence to the established guidelines. Data stewards play a pivotal role in managing and preserving data as a valuable asset or providing guidance on best practices.

Data Custodians: Data custodians are responsible for the technical aspects of data asset onboarding, maintenance, and end-of-life updates. They handle the operational tasks related to data governance, ensuring data is appropriately managed and secured.

Data Governance Committee: This committee serves as the primary forum for approving data policies, standards, and addressing escalated issues. It comprises representatives from various areas of the organization and may include specialized subcommittees dedicated to specific data domains like customer, vendor, product, and employee.

Additionally, organizations may establish a dedicated Data Governance Office with a specialized team to support and coordinate data governance efforts. Here are some key roles that could be part of a Data Governance Team:

Master Data Governance Manager: Responsible for designing, implementing, and maintaining master data control and governance initiatives.

Solution & Data Governance Architect: Provides oversight and guidance for solution designs and implementations related to data governance.

Data Analyst: Utilizes data analytics to identify trends and gain valuable insights.

Data Strategist: Develops and executes strategic plans to leverage data for trend and pattern analysis.

Compliance Specialist: Ensures adherence to required standards, including legal, defense, medical, and privacy regulations.

It is crucial to have well-documented role descriptions, clear expectations, and effective communication channels outlined in a RACI (Responsible, Accountable, Consulted, and Informed) matrix. In summary, the involvement of these stakeholders and the establishment of clear roles and responsibilities are fundamental to successful data governance implementation within an organization.

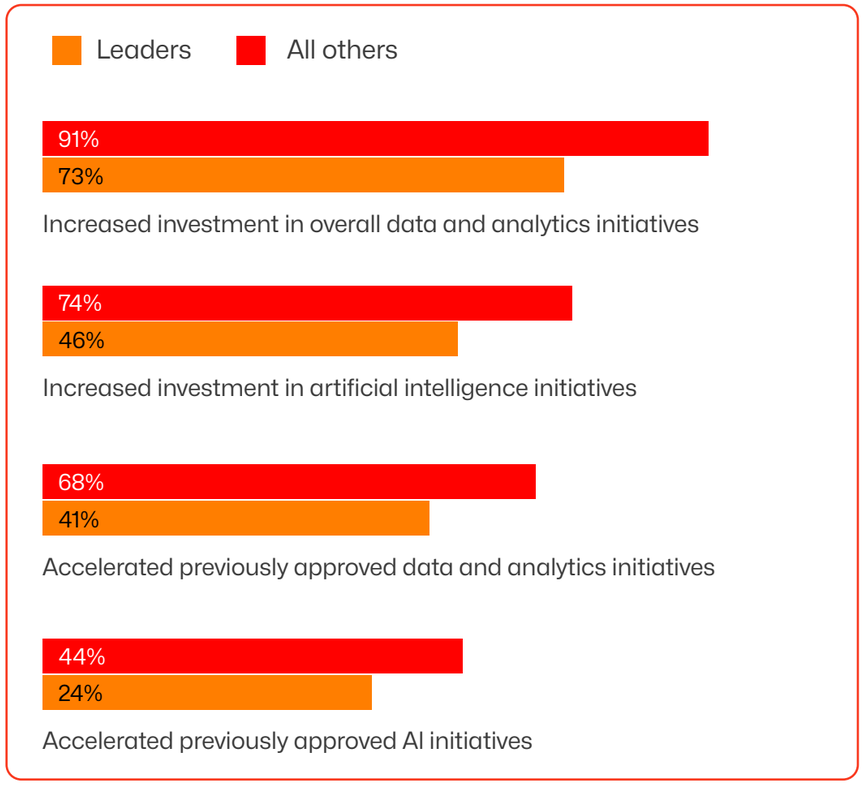
The Data Governance Framework

Expanding Data, Analytics, and Artificial Intelligence

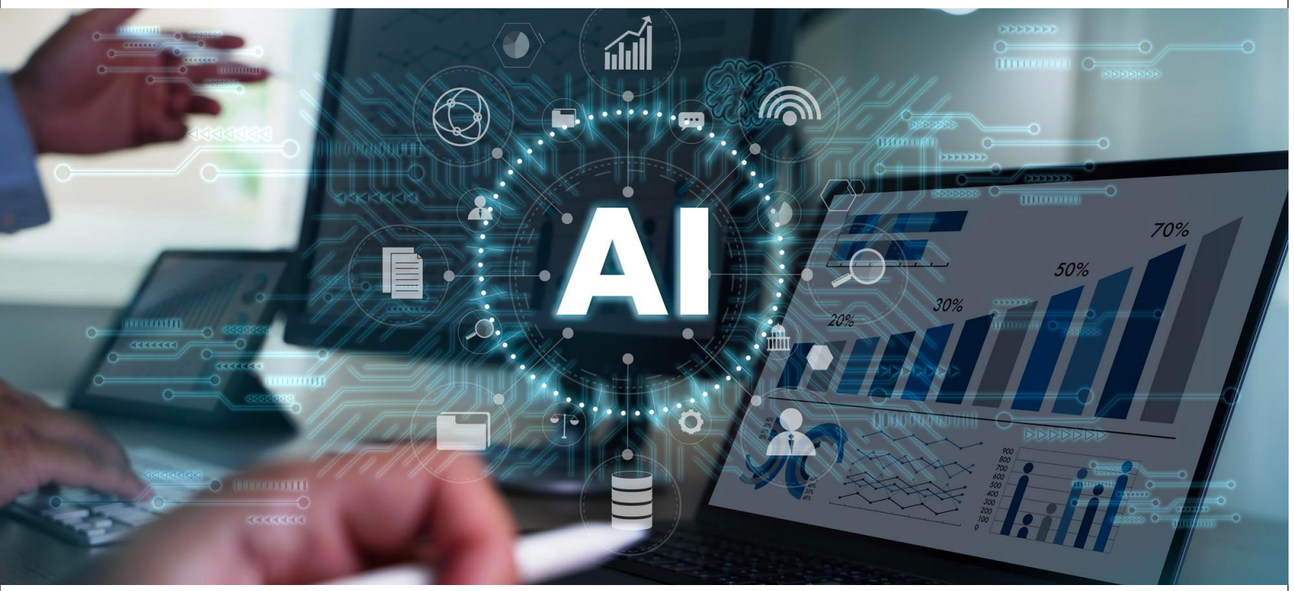
More leaders boosted spending on and accelerated these initiatives

How has your organization's investment in the following initiatives changed in response to disruptions and events of the last two years?

For each of the following types of initiatives, how has their status changed in response to disruptions and events of the last two years? (SELECT ALL THAT APPLY)



Source: Harvard Business Review Analytic Services survey, November 202

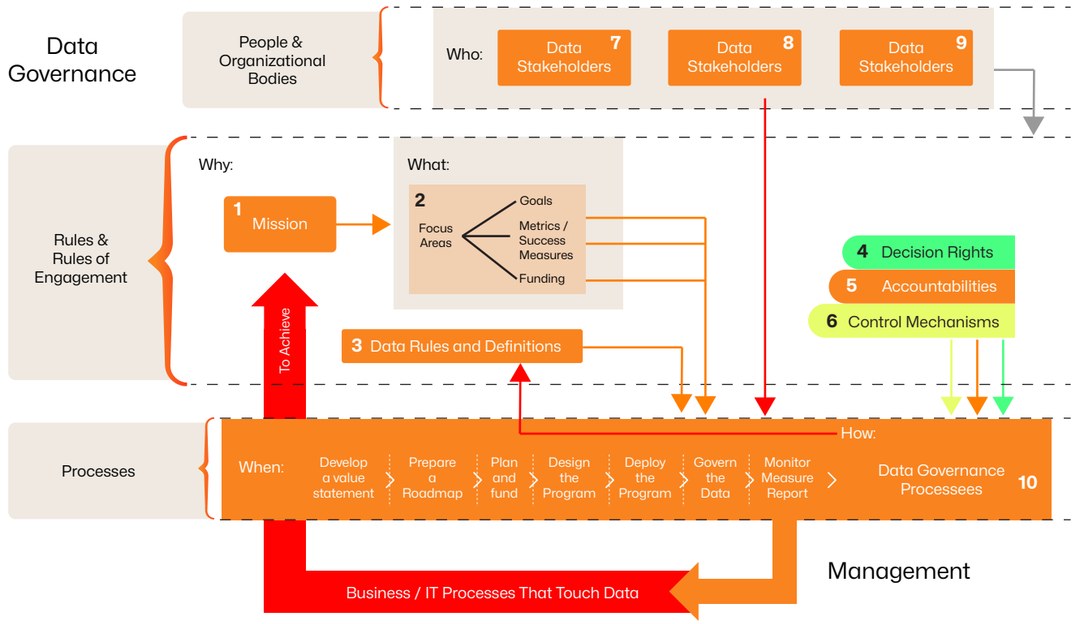


According to a recent report by HRB, effective data-to-value strategies, when coupled with robust data governance practices, can address various critical issues. These include identifying new data sources, exploring opportunities for data deployment and insights, digitizing internal and customer-facing solutions, establishing new roles focused on data and insights, measuring data's economic costs and benefits, and balancing data governance and risk with data availability and innovation.

The report further highlights that leaders who prioritize data governance and have clear enterprise strategies related to data, analytics, and AI are more likely to drive successful outcomes. In fact, 84% of these leaders stated that their organizations have a clear enterprise strategy for managing and extracting value from data, compared to only half of the other respondents.

Organizations can ensure that data is effectively managed, protected, and leveraged to drive business success by implementing robust data governance frameworks and aligning them with data-to-value strategies. Data governance acts as a foundation for enabling data-driven decision-making, mitigating risks, ensuring data quality and integrity, and fostering a culture of data-driven innovation throughout the organization.

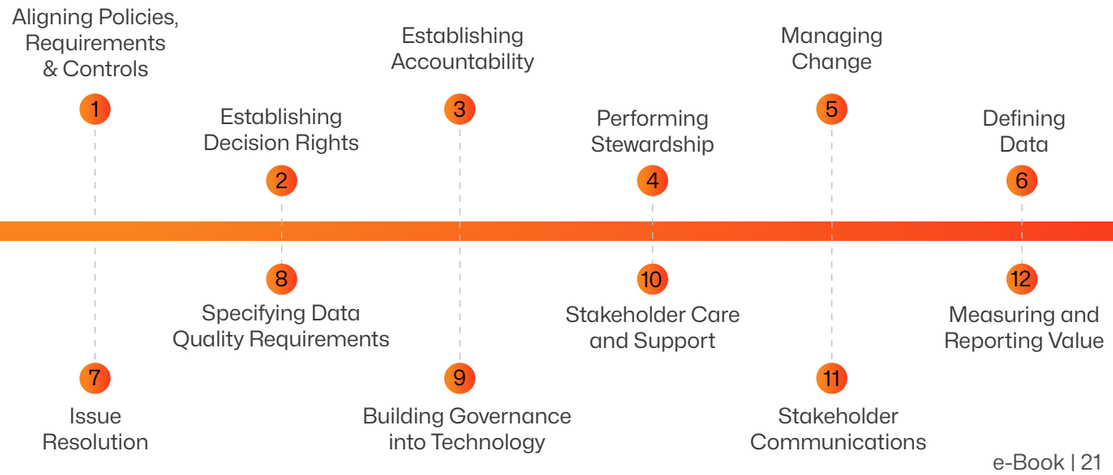
The report's findings underscore the importance of integrating data governance practices into data-to-value strategies to maximize the value and potential of data assets in today's data-driven landscape.



Source: The DGI Data Governance Framework, the Data Governance Institute

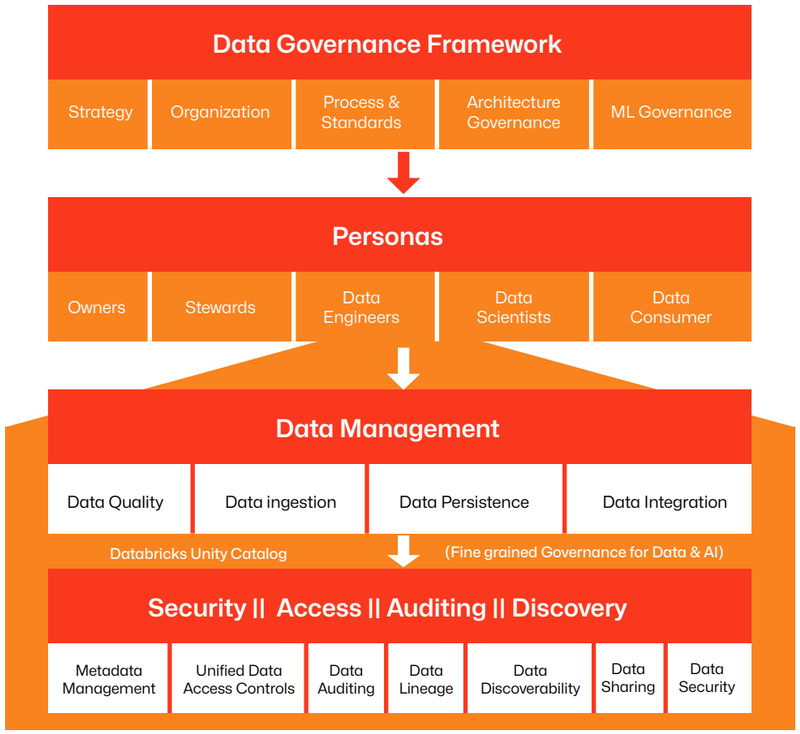
Definition:
Data Governance is the exercise of decision making and authority for data-related matters. It's a system of decision rights and accountabilities for information-related processes, executed according to agreed upon models which describe who can take what actions with what information and under what circumstaces, using what methods.

Processes for governing how data is used, and when, and by whom



Indium's Data Governance Framework with Databricks

Governance with Databricks



Data Governance Framework: Enforces policies, process & standards, practices implemented and to securely manage data assets within the organization

Unity Catalog: Is a unified governance solution for all data and AI assets including files, tables, machine learning models and dashboards in any of the cloud platform in the lakehouse architecture

Data Management: Involves the collection, integration, organization and persistence of trusted data sets and to derive maximum business benefits for the organizations with trusted data set in the lakehouse

Meta Data Management: Centralized Metadata layer (Metastore) represents the organization's information architecture that provides the ability to catalog and share data assets across lakehouse, enterprise regions and clouds.

Unified data access controls: A single and unified permissions model across all data assets and all clouds

Data Auditing: Provides a centralized fine grained auditing capabilities and satisfy the compliance & audit requirements

Data Lineage: Automated & Realtime Data Lineage to get end-to-end visibility and how data flows in lakehouse from source to consumption

Data Discovery: Enabling data teams to easily find data assets across their organization, collaborate on different projects and innovate
quickly and efficiently

Data Sharing: Open solution Data can be shared across clouds and platforms

Elements of a Data Governance Framework

WHY?

Define the purpose and drivers behind your data governance initiative, such as compliance, customer service improvement, or data-driven growth.

WHO?

Identify relevant stakeholders, including Data Owners, Stewards, and a Steering Committee, led by a CDO or Data Governance Manager to ensure data standards and governance are maintained.

WHAT?

Take a progressive approach by selecting specific initial data sources or departments to implement the data governance program. Choose programs wisely based on objectives.

WHEN?

Plan the timing of each element of your data governance strategy, considering team members' readiness and data literacy to avoid disruptions.

WHERE?

Ensure proper data storage practices across the organization, with top-level management allocating storage budgets and individual data owners taking responsibility for data asset protection.

These elements form the foundation of an effective data governance framework, enabling organizations to establish control, standardization, and accountability over their data assets.

Implementing Data Governance with Best Practices

Data Governance Best Practices:

- Start small
- Set clear, measurable goals
- Establish ownership
- Identify roles and responsibilities
- Educate stakeholders
- Focus on the operating model
- Map infrastructure, architecture, and tools
- Develop standardized data definitions
- Identify data domains
- Identify critical data elements
- Define control measurements
- Build a business case
- Leverage metrics
- Communicate frequently
- Emphasize practice over a project

Start small: Begin your data governance journey with manageable and achievable steps. Focus on quick wins and gradually expand your efforts over time.

Set clear and measurable goals: Define specific goals that can be measured to track progress. Celebrate achievements and use them as motivation to pursue the next milestones.

Establish ownership: Ensure the data governance framework has clear business ownership for its successful implementation and sustainability.

Identify roles and responsibilities: Data governance is a collaborative effort involving stakeholders from various parts of the organization. Define and assign specific roles and responsibilities to ensure accountability.

Educate stakeholders: Use business terminology to explain data governance concepts and translate its academic aspects into meaningful business contexts to engage stakeholders effectively.

Focus on the operating model: Integrate the data governance framework seamlessly into your enterprise's business operations and processes.
Map infrastructure, architecture, and tools: Align the data governance framework with your enterprise architecture, IT landscape, and required tools for efficient implementation and management.

Develop standardized data definitions: Strike a balance between centralization and localization by establishing standardized data definitions that enable consistency while allowing flexibility when necessary.

Identify data domains: Focus on the highest impact and effort ratio for improving data governance maturity.

Identify critical data elements: Prioritize and focus on the most critical data elements that have a significant business impact and require stringent governance.

Define control measurements: Implement them within relevant business processes, IT applications, and reporting systems to ensure data quality and compliance.

Build a business case: Articulate the benefits of advancing data governance maturity, such as growth opportunities, cost savings, and risk and compliance management.

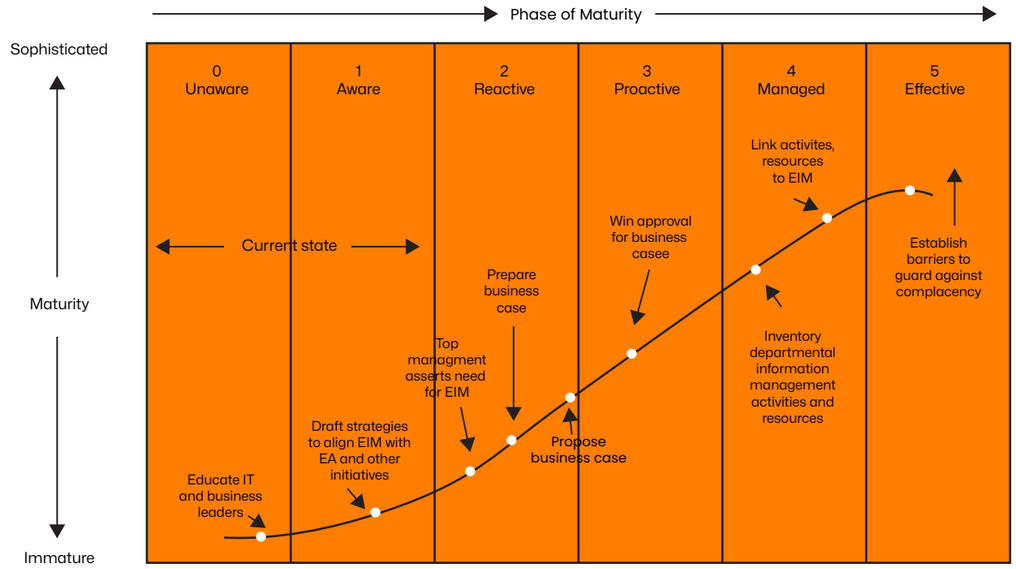
Leverage metrics: Select a limited set of data quality key performance indicators (KPIs) that can be correlated with overall enterprise performance indicators.

Communicate frequently: Effective communication is crucial in data governance. Regularly engage with stakeholders, share updates, and address concerns to foster understanding and support.

Emphasize practice over a project: Recognize that data governance is an ongoing practice rather than a one-time project. Continuously refine and adapt your approach to evolving needs and challenges.

By following these best practices, organizations can enhance their data governance initiatives and unlock the full potential of their data assets.

Where Are You On The Data Governance Maturity Level?



The Gartner Data Governance Maturity Model enables organizations to enhance their information management practices. Let's explore the stages and actions required for effective enterprise information management (EIM).

(Level 0) Unaware

1. There is no governance, security, ownership, or accountability for information or data.
2. There is no official information architecture, philosophy, or method for producing, gathering, distributing, and exchanging information.
3. There are no data models, business glossaries, metadata management, or uniform standards.
4. Most document management, workflow, and archiving are done through email.
5. Across several systems and apps, information is scattered and unreliable.
6. Strategic choices made without sufficient information
7. Architects and strategic planners should inform IT and business leaders about EIM and its potential benefits. Be sure to emphasize the dangers of legal and regulatory problems.

Being alert (level 1)

1. Lack of data ownership is revealed
2. It is acknowledged that EIM lacks business sponsorship.
3. The company begins to recognize the importance of information
4. Information inconsistencies and deteriorating data quality are recognized as problems.
5. It is acknowledged that there is a need for shared standards, principles, processes, and instruments.
6. Business intelligence produces duplicate and contradictory reports. View this free resource on building a report inventory.
7. Risks connected to not having an EIM are listed and assessed.
8. Items for action In accordance with enterprise architecture and company strategic intent, the architecture staff designs the EIM strategy.

Reacting (level 2)

1. Nowadays, business recognizes the value of information.
2. Information about cross-functional projects is exchanged
3. Data and information are beginning to be shared between departments and systems with various owners.
4. Procedures for information quality are still reactive.
5. Although information management policies and standards are developed, there is little compliance.
6. Metrics are gathered, and a baseline evaluation is created, primarily emphasizing data and information preservation.
7. Action items: Upper management should advocate EIM to resolve problems with cross-functional information. EIM's value proposition has been assembled and presented.

(Level 3) proactive

1. Information owners and stewards are tasked with managing this asset since it is thought to be required to support decisions.
2. The ability to share information is essential to facilitating enterprise-wide projects.
3. The operating concept and governance roles are formalized.
4. Complete adherence to information management policies and guidelines.
5. Every project involving development and deployment includes data governance. Reduced operational risk is achieved.
6. Taking action: Create and present the management and stakeholders with the EIM business case. Find departmental or unit-level EIM possibilities.

(Level 4) Managed

1. Information is seen as crucial.
2. The enterprise's information policies and standards have been defined, implemented, and are widely understood.
3. A governing body has been established to address cross-functional information concerns and pinpoint best practices.
4. Through dashboards, measurements are established, information assets are categorized, productivity measures are created, and metrics are communicated.
5. Action items: It is necessary to inventory information management tasks and projects and confirm that they align with the EIM strategy. Make a balanced scorecard for managing information.

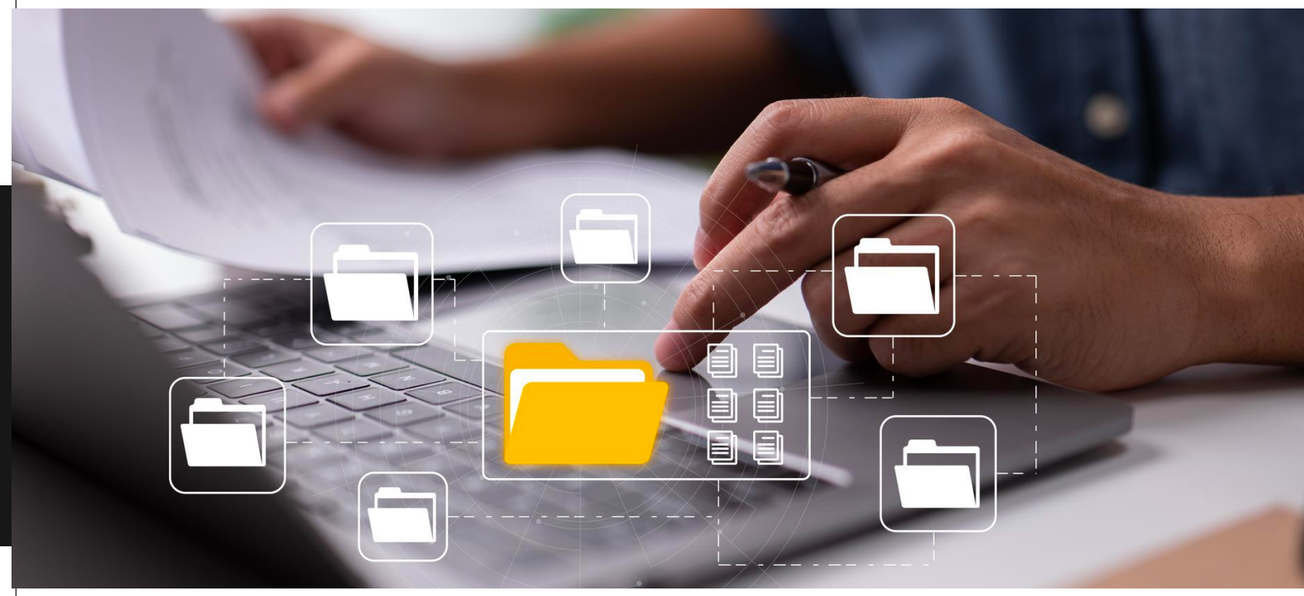
Successful (level 5)

1. Information management provides value and efficiency and is viewed as a competitive advantage.
2. There are in place service level agreements.
3. EIM strategies focus on reducing risks and hitting or exceeding productivity goals.
4. All enterprise-wide information activities are coordinated by the well-organized EIM organization.
5. The company's EIM objectives were met.
6. Implement controls and procedures that guarantee information excellence, even if the company's leadership or direction changes.

Takeaway: Their methodology emphasizes that EIM is a program incorporating ongoing activities rather than a single project. To secure ongoing support and resources, leadership must comprehend and embrace this message from the outset. It is unacceptable to skip a phase or the activities that accompany it because doing so would result in EIM failure and increased risks and expenses in the future. Most businesses are still developing their EIM systems, as you might anticipate.

Assessing Data Maturity: Maturity Model Questionnaire

1. How is the data stored within the organization?
2. What is the level of accessibility to the required data?
3. Is all the source systems' data integrated, or is data kept in silos?
4. What is the level of data quality maintained within the current system?
5. What is the frequency of data being fetched?
6. What is the level of granularity of data maintained within the source systems?
7. Are the historical data requirements and archival needs well-defined and maintained?
8. How well is the documentation around the data needs?
9. What are the data-level protection and privacy standards maintained in the current system?



Importance of Data Security and Privacy in the Modern Enterprise

Data security and privacy have become paramount for enterprises in the modern digital landscape. The vast amount of data collected and processed by organizations hold immense value, but it also presents significant risks if not adequately protected. Here are a few reasons why data security and privacy are crucial:

Preventing Data Breaches:
Data breaches can result in severe financial and reputational damage to enterprises. According to the 2021 Cost of a Data Breach Report by IBM Security and Ponemon Institute, the average cost of a data breach reached a staggering $4.24 million per incident globally. Protecting sensitive data minimizes the likelihood of breaches and their associated

Safeguarding Customer Trust:
Data breaches and privacy violations erode customer trust. A survey conducted by Deloitte in 2021 revealed that 73% of consumers are more concerned about data privacy than the previous year. Enterprises can maintain customer loyalty and enhance their brand reputation by prioritizing data security and

Compliance with Regulations:
Governments worldwide have introduced data privacy regulations to protect individuals' rights and hold organizations accountable for their data handling practices. Non-compliance with these regulations can lead to hefty fines and legal consequences. For example, the General Data Protection Regulation (GDPR) has imposed penalties of up to €20 million or 4% of global annual turnover, whichever is higher, for

Overview of Data Security Best Practices

Implementing data security best practices helps organizations establish robust safeguards against threats and vulnerabilities. Some key practices include:

1. Access Control: Limiting access to data based on the principle of least privilege helps prevent unauthorized individuals from accessing sensitive information.
2. Encryption: Encrypting data at rest and in transit provides additional protection. Encrypted data is significantly more challenging to exploit in a breach.
3. Regular Patching and Updates: Keeping software, operating systems, and applications up to date with the latest patches ensures that known vulnerabilities are addressed promptly.
4. Employee Education and Awareness: Training employees about data security risks, best practices, and social engineering techniques helps mitigate the human factor, which is often a weak link in security.

Understanding Data Privacy Regulations and Compliance Requirements

Several data privacy regulations have emerged globally to safeguard individuals' privacy rights. The following regulations are among the most notable:

1. General Data Protection Regulation (GDPR): Implemented by the European Union, GDPR gives individuals control over their personal data and imposes obligations on organizations handling such data.
2. California Consumer Privacy Act (CCPA): CCPA grants California residents rights over their personal information and requires businesses to disclose their data collection and usage practices.

Compliance with these regulations involves various requirements, such as obtaining consent, ensuring data subject rights, and implementing privacy by design principles. Organizations must understand and adhere to the regulations applicable to their operations to avoid penalties and maintain compliance.

Strategies for Protecting Sensitive Data and Mitigating Security Risks

To protect sensitive data and mitigate security risks effectively, organizations should consider the following strategies:

1. Implement Data Classification: Categorize data based on sensitivity and define appropriate security controls for each category. This allows for targeted protection measures based on the level of risk associated with different types of data.
2. Regular Vulnerability Assessments and Penetration Testing: Conducting assessments helps identify vulnerabilities and weaknesses in systems, allowing organizations to address them promptly.
3. Incident Response and Disaster Recovery Planning: Establish a robust incident response plan to effectively address security incidents. Additionally, implement disaster recovery procedures to restore systems and data in case of a breach or loss.
4. Continuous Monitoring: Implement systems and processes for monitoring network activity, user behavior, and potential threats. This enables the identification of anomalous activities and timely response to potential security incidents.

In conclusion, data security and privacy are critical for modern enterprises to protect against data breaches, maintain customer trust, and comply with regulations. By implementing data security best practices, understanding privacy regulations, and adopting effective strategies, organizations can safeguard sensitive data and mitigate security risks effectively.

Indium's Recommendation

Based on recommendations from our experts, implementing effective data governance initiatives or programs can be facilitated by following these tips:

1. **Secure Management Support:** Ensure that your data governance program has strong support from management to drive its success.
2. **Embrace an Iterative Approach:** View data governance as a continuous and iterative process, consisting of sub-projects rather than a one-time big bang initiative.
3. **Start with Pilot Projects:** Begin with small-scale pilot projects to gain valuable experience and insights that can be applied across the organization.
4. **Time-Bound Projects:** While data governance programs may span years, individual projects should have specific time frames and not exceed three months to maintain momentum and focus.
5. **Define Clear Objectives:** Set well-defined and meaningful targets that align with your organization's data governance goals.
6. **Gain Stakeholder Acceptance:** Prioritize stakeholder involvement and ensure transparency throughout the data governance process. Open communication without hidden agendas is key.
7. **Leverage Existing Resources:** Utilize templates, models, best practices, and available market tools, frameworks, libraries, or consultants rather than reinventing the wheel.
8. **Appoint Suitable Roles:** Properly assign organizational roles, emphasizing effective communication skills for the program manager to navigate political dynamics.
9. **Streamline Established Processes:** Evaluate existing processes and solutions to identify areas where streamlining and optimization are needed.
10. **Evaluate Data Governance Platforms:** Assess and select platforms that align with your organization's requirements and support your data governance objectives.
11. **Establish Clear Structures:** Create well-defined structures and responsibilities within the data governance program to ensure clarity and accountability.
12. **Document Best Practices:** Develop a comprehensive methodology for documenting and sharing organizational best practices related to data governance.

By incorporating these recommendations into your data governance initiatives, you can enhance the effectiveness and success of your data governance program, leading to improved data management, quality, and value realization within your organization.

Notes

Gartner. (2023). Choose Adaptive Data Governance over One-Size-Fits-All for Greater Flexibility. Retrieved from https://www.gartner.com/en/articles/choose-adaptive-data-governance-over-one-size-fits-all- for- greater-flexibility

ODI. (2023). International Data Assurance: Market Briefing. Retrieved from https://www.theodi.org/article/international-data-assurance-market-briefing/

Microsoft. (n.d.). Harvard Business Review Analytic Services Research Report. Retrieved from https://info.microsoft.com/ww-landing-harvard-business-review-analytic-services-research-report.html

Metia Group. (2023). Metia Group Research for Open Data Institute Reveals Global Data Assurance Market Opportunities. Retrieved from https://metia.com/news/metia-group-research-for-open-data-institute-reveals-global-data-assurance-market-opportunities/

Gartner. (n.d.). Best Practices for Data and Analytics Governance. Retrieved from https://www.gartner.com/en/documents/846312

For more information, please contact

Srikanth Manoharan
Executive Vice President
QA Digital Assurance
Americas, Asia, Europe, Australasia
srikanth.manoharan@indiumsoft.com

Krishnakumar Aravamudhan
Vice President - Data Management
krishnakumar.aravamudhan@indiumsoft.com

Arunachalam Sankaralingam
Vice President - Digital Assurance
arunachalam.s@indiumsoft.com

Rajavel G Kanagavelu
Senior Data Architect - Data Management
rajavel.kanagavelu@indiumsoft.com

About the Authors

Srikanth Manoharan
srikanth.manoharan@indiumsoft.com

Srikanth Manoharan, Executive Vice President (EVP) at Indium Software, is a visionary and trailblazer leading the Digital Assurance portfolio, propelling the company to new heights of excellence. Mano has pioneered and nurtured the “Data Assurance” practice, cultivating it with diverse talents and innovative offerings. He embodies extensive experience and expertise in “Quality Engineering,” earning recognition as one of the industry’s true veterans. Mano’s unwavering passion is dedicated to helping customers uncover and tackle their data quality challenges, making him an indispensable asset in the ever-evolving landscape of digital assurance.

Arunachalam Sankaralingam, Vice President of Digital Assurance at Indium Software, is a certified professional with extensive experience in systems validation and project management. He coordinates testing activities and ensures compliance with clients’ validation requirements. With a technical background encompassing web applications, database testing, and automation using VBA, QTP, RRAFS, and more, Arunachalam is a versatile expert ready to share his insights with professionals seeking to enhance their data-centric testing strategies.

Arunachalam Sankaralingam
arunachalam.s@indiumsoft.com

About the Authors

Krishnakumar Aravamudhan
krishnakumar.aravamudhan@indiumsoft.com

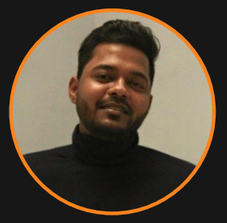
Krishnakumar Aravamudhan, a distinguished professional in the field of data and analytics, serves as Vice President of Data Management. With a wealth of experience and expertise, Krishnakumar has been instrumental in shaping data strategies that drive business success. His visionary leadership and commitment to excellence have made him a prominent figure in the data management arena.

Jayalakshmi Srinivasan
jayalakshmi.srinivasan@indiumsoft.com

Jayalakshmi Srinivasan is a seasoned data and analytics professional with a remarkable 12+ years of experience, having successfully operated both on-site and offshore. She has adeptly overseen projects and programs within the data and analytics realm, specializing in the banking and retail sectors. Jayalakshmi's passion lies in exploring and harnessing the power of data, continually upgrading her expertise in this dynamic technological landscape.

Rajavel Kanagavelu
rajavel.kanagavelu@indiumsoft.com

With over 20 years in the IT industry, Rajavel Kanagavelu's expertise lies in Microsoft Technologies, particularly within Data Analytics and Data Engineering, spanning both On-Premise and Cloud environments. His track record includes architecting solutions, managing practices, and delivering successful projects across diverse domains, embodying roles from solution architect to CoE leadership.



Abishek Balakumar
abishek.balakumar@indiumsoft.com

Abishek Balakumar is a Tech Marketing Visionary and a Strategic Marketing Consultant specializing in Banking and Financial Services. As a seasoned Partner Marketer, he leverages his expertise to host engaging podcasts and webinars. With a keen focus on APAC and US event management, he is a specialist and enabler in orchestrating successful business events. Abishek is also a gifted Business Storyteller and an accomplished Author, holding a master's degree in Marketing and Data & Analytics.

About Indium

Indium is an AI-driven digital engineering company that helps enterprises build, scale, and innovate with cutting-edge technology. We specialize in custom solutions, ensuring every engagement is tailored to business needs with a relentless customer-first approach. Our expertise spans Generative AI, Product Engineering, Intelligent Automation, Data & AI, Quality Engineering, and Gaming, delivering high-impact solutions that drive real business impact.

With 5,000+ associates globally, we partner with Fortune 500, Global 2000, and leading technology firms across Financial Services, Healthcare, Manufacturing, Retail, and Technology–driving impact in North America, India, the UK, Singapore, Australia, and Japan to keep businesses ahead in an AI-first world.

USA

Cupertino | Princeton

Toll-free: +1-888-207-5969

INDIA

Chennai | Bengaluru | Mumbai | Hyderabad | Pune

Toll-free: 1800-123-1191

UK

London

Ph: +44 1420 300014

SINGAPORE

Singapore

Ph: +65 6812 7888

www.indium.tech

For Sales Inquiries
sales@indium.tech

For General Inquiries
info@indium.tech